

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: THỰC TẬP CƠ SỞ  
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.6  
PHÂN TÍCH LOG HỆ THỐNG**

Sinh viên thực hiện:

B22DCAT253    Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC.....	2
<b>CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH.....</b>	<b>4</b>
1.1 Mục đích.....	4
1.2 Ý nghĩa của một số lệnh dùng cho quá trình phân tích log.....	4
<b>1.2.1 grep.....</b>	<b>4</b>
1.2.1.1 Mô tả: .....	4
1.2.1.2 Cú pháp: .....	4
1.2.1.3 Ví dụ:.....	4
1.2.1.4 Tùy chọn hữu ích: .....	4
<b>1.2.2 gawk (GNU AWK) .....</b>	<b>4</b>
1.2.2.1 Mô tả: .....	4
1.2.2.2 Cú pháp: .....	4
1.2.2.3 Ví dụ:.....	4
1.2.2.4 Tính năng hữu ích: .....	5
<b>1.2.3 find .....</b>	<b>5</b>
1.2.3.1 Mô tả: .....	5
1.2.3.2 Cú pháp: .....	5
1.2.3.3 Ví dụ:.....	5
1.2.3.4 Ứng dụng:.....	5
<b>1.2.4 secure (Tập /var/log/secure) .....</b>	<b>5</b>
1.2.4.1 Mô tả: .....	5
1.2.4.2 Cú pháp phân tích:.....	5
1.2.4.3 Ứng dụng:.....	5
<b>1.2.5 access_log (Tập /var/log/apache2/access.log hoặc /var/log/nginx/access.log) .....</b>	<b>6</b>
1.2.5.1 Mô tả: .....	6
1.2.5.2 Cách phân tích:.....	6
1.2.5.3 Ứng dụng:.....	6
<b>1.2.6 Tổng kết.....</b>	<b>6</b>
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH .....</b>	<b>7</b>
2.1 Chuẩn bị môi trường .....	7
2.2 Các bước thực hiện.....	7
<b>2.2.1 Phân tích log sử dụng grep trong Linux .....</b>	<b>7</b>
2.2.1.1 Quét cổng với Zenmap trên Kali .....	7

2.2.1.2 Kiểm tra nội dung website bằng curl .....	8
2.2.1.3 Kiểm tra file access_log trên máy nạn nhân .....	9
<b>2.2.2 Phân tích log sử dụng gawk trong Linux .....</b>	<b>10</b>
2.2.2.1 Tạo tài khoản mới trên máy Linux Internal Victim .....	10
2.2.2.2 Kiểm tra file log trên máy Linux Internal Victim .....	11
2.2.2.3 Truy vấn log từ máy Kali Attack .....	12
<b>2.2.3 Phân tích log sử dụng find trong Windows.....</b>	<b>14</b>
2.2.3.1 Sử dụng xHydra để brute-force FTP .....	14
2.2.3.2 Phân Tích Log FTP trên Windows Server 2019 .....	15
<b>KẾT LUẬN .....</b>	<b>16</b>
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>16</b>

# CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

## 1.1 Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, bao gồm:

- Phân tích log sử dụng grep/gawk trong Linux
- Phân tích log sử dụng find trong Windows
- Tìm hiểu về Windows Event Viewer và auditing
- Phân tích event log trong Windows

## 1.2 Ý nghĩa của một số lệnh dùng cho quá trình phân tích log

Dưới đây là ý nghĩa và công dụng của một số lệnh phổ biến trong quá trình phân tích log trên hệ điều hành Linux:

### 1.2.1 grep

#### 1.2.1.1 Mô tả:

Lệnh grep dùng để tìm kiếm các dòng có chứa một chuỗi hoặc một mẫu (pattern) trong tệp tin hoặc đầu ra của lệnh khác.

#### 1.2.1.2 Cú pháp:

```
grep [tùy chọn] "chuỗi_cần_tìm" tệp_log
```

#### 1.2.1.3 Ví dụ:

Tìm các dòng có chứa từ “error” trong tệp syslog:

```
grep "error" /var/log/syslog
```

#### 1.2.1.4 Tùy chọn hữu ích:

- -i: Không phân biệt chữ hoa/chữ thường
- -r: Tìm kiếm đệ quy trong thư mục
- -n: Hiển thị số dòng

### 1.2.2 gawk (GNU AWK)

#### 1.2.2.1 Mô tả:

gawk là phiên bản mở rộng của awk, dùng để xử lý và phân tích dữ liệu dạng văn bản theo cột.

#### 1.2.2.2 Cú pháp:

```
gawk '{câu_lệnh_xử_ly}' tệp_log
```

#### 1.2.2.3 Ví dụ:

Lấy cột thứ 1 và 4 trong tệp log access.log:

```
gawk '{print $1, $4}' /var/log/apache2/access.log
```

#### 1.2.2.4 Tính năng hữu ích:

- Chia nhỏ log thành các cột để xử lý dễ dàng hơn
- Có thể kết hợp với grep, sort, uniq để phân tích sâu hơn

### 1.2.3 find

#### 1.2.3.1 Mô tả:

Dùng để tìm kiếm tệp tin trong hệ thống theo tên, thời gian chỉnh sửa, kích thước, v.v.

#### 1.2.3.2 Cú pháp:

```
find [thư_mục] [tùy_chọn] [điều_kiện]
```

#### 1.2.3.3 Ví dụ:

- Tìm tất cả các tệp log trong /var/log:  

```
find /var/log -name "*.log"
```
- Tìm các tệp log được chỉnh sửa trong 7 ngày qua:  

```
find /var/log -name "*.log" -mtime -7
```

#### 1.2.3.4 Ứng dụng:

- Tìm kiếm nhanh các tệp log để phân tích
- Xóa các tệp log cũ để tiết kiệm dung lượng

### 1.2.4 secure (Tệp /var/log/secure)

#### 1.2.4.1 Mô tả:

Đây là tệp log chứa thông tin về xác thực, đăng nhập, SSH, và quyền root trên hệ thống Linux.

#### 1.2.4.2 Cú pháp phân tích:

- Kiểm tra đăng nhập thất bại:  

```
grep "Failed password" /var/log/secure
```
- Xem các lần đăng nhập SSH thành công:  

```
grep "Accepted password" /var/log/secure
```

#### 1.2.4.3 Ứng dụng:

- Theo dõi bảo mật hệ thống
- Phát hiện các cuộc tấn công brute-force

### **1.2.5 access\_log (Tập /var/log/apache2/access.log hoặc /var/log/nginx/access.log)**

#### **1.2.5.1 Mô tả:**

Đây là tệp log ghi lại tất cả các yêu cầu HTTP đến máy chủ web Apache/Nginx.

#### **1.2.5.2 Cách phân tích:**

- Xem 10 yêu cầu gần nhất:

```
tail -n 10 /var/log/apache2/access.log
```

- Đếm số lượt truy cập từ một IP cụ thể:

```
grep "192.168.1.100" /var/log/apache2/access.log | wc -l
```

- Lấy danh sách các IP truy cập nhiều nhất:

```
awk '{print $1}' /var/log/apache2/access.log | sort | uniq -c | sort -nr | head
```

#### **1.2.5.3 Ứng dụng:**

- Theo dõi lượng truy cập vào website
- Phát hiện các cuộc tấn công DDoS

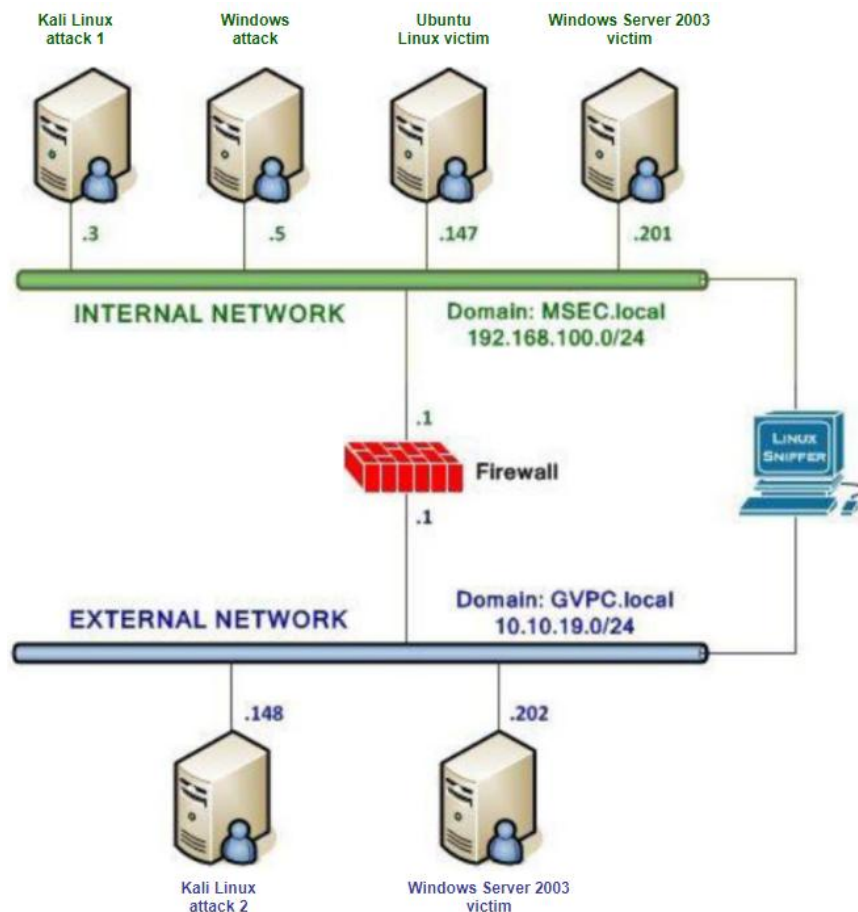
### **1.2.6 Tổng kết**

<b>Lệnh</b>	<b>Công dụng chính</b>
<b>grep</b>	Tìm kiếm trong log
<b>gawk</b>	Xử lý và phân tích dữ liệu theo cột
<b>find</b>	Tìm kiếm tệp log theo điều kiện
<b>secure</b>	Log về xác thực và SSH
<b>access_log</b>	Log về truy cập web

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation (hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5.

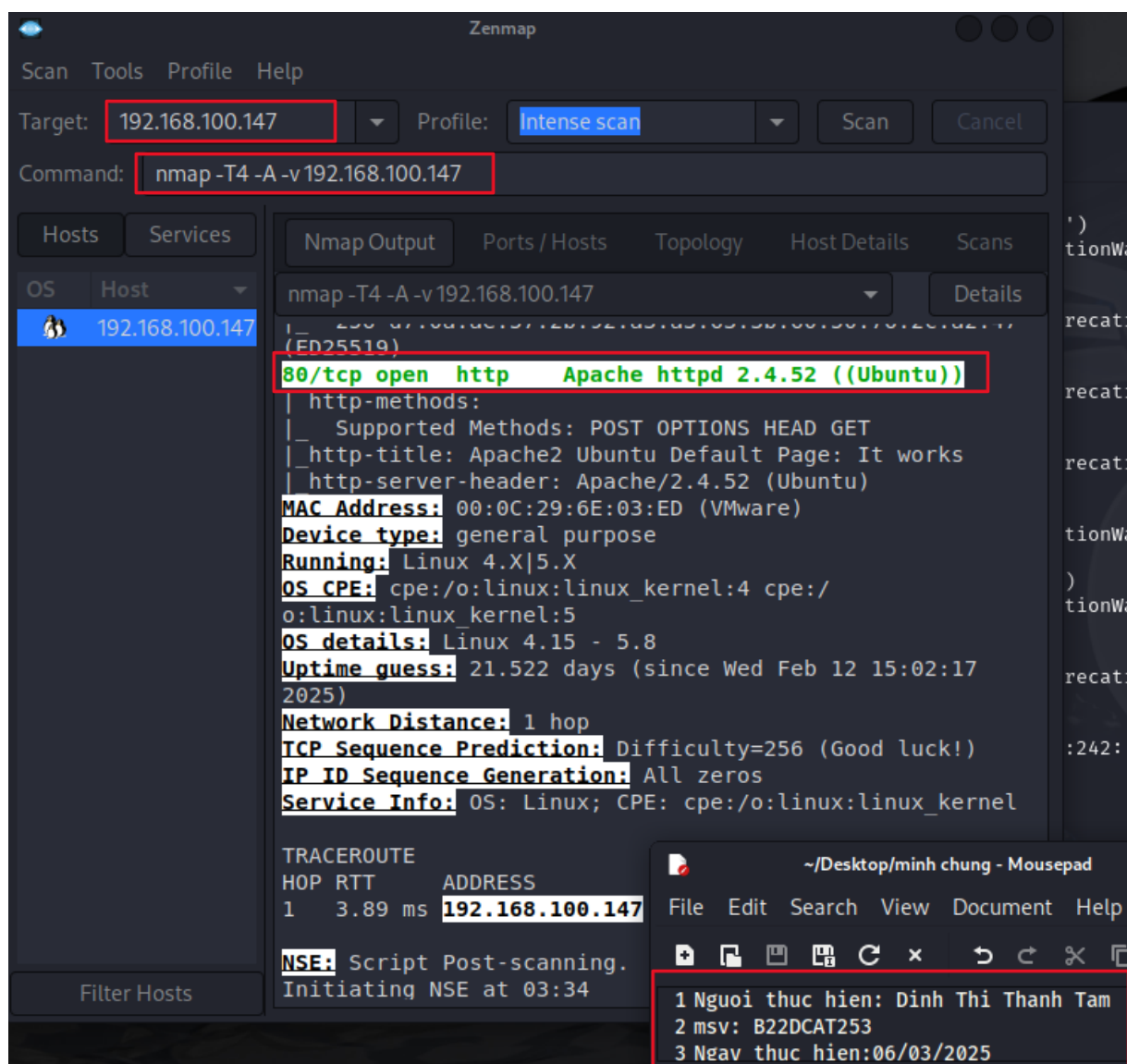


### 2.2 Các bước thực hiện

#### 2.2.1 Phân tích log sử dụng grep trong Linux

##### 2.2.1.1 Quét cổng với Zenmap trên Kali

- Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147 (Máy Linux victim)
  - Nhập vào ô Target: 192.168.100.147
  - Nhập vào ô Command: nmap -T4 -A -v 192.168.100.147
  - Nhấn Scan để bắt đầu quét.
  - Nếu thấy cổng 80/tcp mở với Apache/2.4.52, tiếp tục bước tiếp theo.

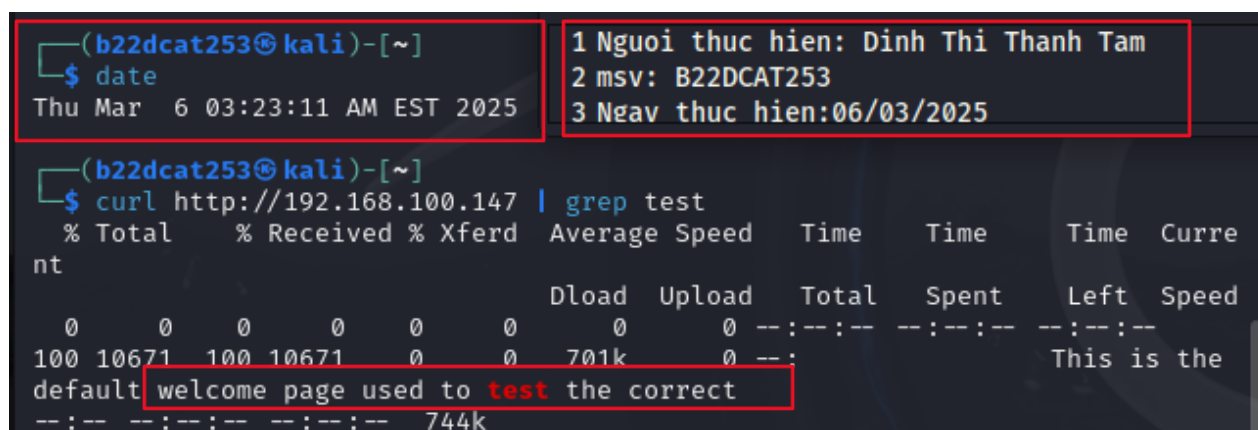


### 2.2.1.2 Kiểm tra nội dung website bằng curl

- Mở terminal trên Kali và chạy:

`curl http://192.168.100.147 | grep test`

➔ Nếu có từ khóa "test", tiếp tục bước tiếp theo.





### 2.2.1.3 Kiểm tra file access\_log trên máy nạn nhân

- Trên máy Linux nạn nhân, mở terminal và di chuyển đến thư mục chứa log của Apache:

```
cd /var/log/apache2
```

- Liệt kê các file log:

```
ls -l
```

```
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ cd /var/log/apache2
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$ date
Thứ năm, 06 Tháng 3 năm 2025 15:30:12 +07
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$ ls -l
total 16
-rw-r----- 1 root adm 8918 Thg 3  6 15:23 access.log
-rw-r----- 1 root adm 1704 Thg 3  6 15:21 error.log
-rw-r----- 1 root adm  0 Thg 3  6 10:22 other_vhosts_access.log
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$
```

Open [ ] \*minh chung ~/

1 Người thực hiện: Dinh Thi Thanh Tam  
2 MSV: B22DCAT253  
3 Ngày thực hiện: 06/03/2025

- Mở file access\_log để kiểm tra các request:

```
cat access.log | grep "curl"
```

```
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$ cat access.log | grep "curl"
192.168.197.144 - - [06/Mar/2025:10:57:14 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.11.0"
192.168.100.3 - - [06/Mar/2025:15:23:42 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.11.0"
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$ date
Thứ năm, 06 Tháng 3 năm 2025 15:36:09 +07
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/apache2$
```

Open [ ] Save

1 Người thực hiện: Dinh Thi Thanh Tam  
2 MSV: B22DCAT253  
3 Ngày thực hiện: 06/03/2025

- Dòng log này cho thấy có một request từ IP 192.168.100.3 truy cập vào server Apache bằng lệnh curl. Cụ thể:
  - Thời gian: 06/Mar/2025 15:23:42
  - Phương thức HTTP: GET / HTTP/1.1
  - Mã phản hồi: 200 (thành công)

- Kích thước response: 10926 bytes
- User-Agent: "curl/8.11.0" (tức là request được gửi từ curl phiên bản 8.11.0)
- Khi đã mở được file access\_log trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm ví dụ: Nmap, Firefox, curl, ...

```

dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-...
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "GET /favicon.ico HTTP/1.1" 404 4
57 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
dinhthithanh tam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine: /var/log/ap
ache$ cat access.log | grep "Nmap"Firefox
1
2
3
4
1 Người thực hiện: Dinh Thi Thanh Tam
2 MSV: B22DCAT253
3 Ngày thực hiện: 06/03/2025
4

```

➔ Minh chứng: ảnh trên là minh chứng kết quả lọc dữ liệu dùng grep trên file log của máy nạn nhân, trong ảnh chụp có phần tên máy có chứa tên và mã sinh viên.

## 2.2.2 Phân tích log sử dụng gawk trong Linux

### 2.2.2.1 Tạo tài khoản mới trên máy Linux Internal Victim

- Trên máy Kali Attack, thực hiện kết nối SSH đến Linux Internal Victim:

*ssh user@IP\_VICTIM*

```
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine: ~
File Actions Edit View Help
^C
— 192.168.100.147 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 2.983/3.540/4.027/0.438 ms

(b22dcat253@kali)-[~]
$ ssh dinhthithanhtam-b22dcat253@192.168.100.147
dinhthithanhtam-b22dcat253@192.168.100.147's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Mar  6 11:22:28 2025 from 192.168.197.144
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$
```

- Sau khi đăng nhập thành công, tạo một tài khoản mới:

`sudo useradd -m <tên_sinh_viên>`

`sudo passwd <tên_sinh_viên>`

```
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ sudo
useradd -m dinhthithanhtam
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ sudo
passwd dinhthithanhtam
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$
```

```
1 Người thực hiện: Dinh Thi Thanh Tam
2 msv: B22DCAT253
3 Ngày thực hiện: 04/03/2025
4 === day la may kali linux===
5
```

- Nhập mật khẩu tùy chọn hai lần để xác nhận.

- Thay đổi mật khẩu cho tài khoản mới

`sudo passwd <tên_sinh_viên>`

- Nhập mật khẩu mới và xác nhận.

#### 2.2.2.2 Kiểm tra file log trên máy Linux Internal Victim

- Các tệp log quan trọng liên quan đến tài khoản người dùng thường nằm trong /var/log/, sử dụng lệnh sau để xem:

`sudo cat /var/log/auth.log | grep "new user"`

The image shows a terminal window with the following commands and output:

```
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ whoami
dinhthithanhtam-b22dcat253
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ date
Thứ năm, 06 Tháng 3 năm 2025 11:30:26 +07
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$ sudo cat /var/log/auth.log | grep "new user"
[sudo] password for dinhthithanhtam-b22dcat253:
Mar  6 11:25:02 dinhthithanhtamb22dcat253-virtual-machine useradd[7631]: new user:
name=b22dcat253, UID=1001, GID=1001, home=/home/b22dcat253, shell=/bin/sh, from=/dev/pts/2
Mar  6 11:25:16 dinhthithanhtamb22dcat253-virtual-machine useradd[7640]: new user:
name=dinhthithanhtam, UID=1002, GID=1002, home=/home/dinhthithanhtam, shell=/bin/sh, from=/dev/pts/2
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:~$
```

Below the terminal, a file manager window shows the contents of a file named `*mi...`:

```
1 Người thực hiện: Dinh Thi Thanh Tam
2 MSV: B22DCAT253
3 Ngày thực hiện: 06/03/2025
```

- Kết quả log hiển thị:
  - User b22dcat253 được tạo (UID=1001, GID=1001, home /home/b22dcat253, shell /bin/sh)
  - User dinhthithanhtam được tạo (UID=1002, GID=1002, home /home/dinhthithanhtam, shell /bin/sh)
  - Cả hai tài khoản được tạo từ /dev/pts/2, nghĩa là quá trình tạo tài khoản có thể được thực hiện từ một phiên terminal từ xa.
- Nhận xét và đánh giá
  - Việc tạo hai tài khoản mới xuất hiện trong file /var/log/auth.log, đây là bằng chứng hệ thống về việc thêm user.
  - Các tài khoản này có UID khác nhau, cho thấy chúng được tạo như người dùng mới thay vì ghi đè tài khoản cũ.
  - Log cho biết user mới được tạo từ /dev/pts/2, thường là một phiên SSH hoặc terminal từ xa.

### 2.2.2.3 Truy vấn log từ máy Kali Attack

- Từ máy Kali, dùng SSH để truy vấn file log trên Linux Internal Victim:  
`ssh user@IP_VICTIM "cat /var/log/auth.log | grep '<tên_sinh_viên>'"`

```
Mar 6 10:15:16 dinhthithanhtam-b22dcat253-virtual-machine systemd: pam_unix(systemd-user:session): session opened for user gdm(uid=128) by (uid=0)
Mar 6 10:15:32 dinhthithanhtam-b22dcat253-virtual-machine polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus name :1.40 [/usr/bin/gnome-keyring-daemon])
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: gkr-pam: unable to locate daemon control file
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: gkr-pam: stubbed password to try later in open session
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: pam_unix(gdm-password:session): session opened for user dinhthithanhtam-b22dcat253(uid=1000) by (uid=0)
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine systemd-logind[948]: New session 2 of user dinhthithanhtam-b22dcat253.
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine systemd: pam_unix(systemd-user:session): session opened for user dinhthithanhtam-b22dcat253(uid=1000) by (uid=0)
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine CRON[1697]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 6 10:17:01 dinhthithanhtam-b22dcat253-virtual-machine CRON[1697]: pam_unix(cron:session): session closed for user root
Mar 6 10:17:02 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Mar 6 10:17:04 dinhthithanhtam-b22dcat253-virtual-machine gnome-keyring-daemon[1713]: The Secret Service was already initialized
Mar 6 10:17:05 dinhthithanhtam-b22dcat253-virtual-machine gnome-keyring-daemon[1713]: The PKCS#11 component was already initialized
Mar 6 10:17:05 dinhthithanhtam-b22dcat253-virtual-machine gnome-keyring-daemon[1713]: The SSH agent was already initialized
Mar 6 10:17:09 dinhthithanhtam-b22dcat253-virtual-machine polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.77 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Mar 6 10:17:24 dinhthithanhtam-b22dcat253-virtual-machine gdm-launch-environment: pam_unix(gdm-launch-environment:session): session closed for user gdm
Mar 6 10:17:24 dinhthithanhtam-b22dcat253-virtual-machine systemd-logind[948]: Session c1 logged out. Waiting for processes to exit.
Mar 6 10:17:25 dinhthithanhtam-b22dcat253-virtual-machine polkitd(authority=local): Unregistered Authentication Agent for unix-session:c1 (system bus name :1.40, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Mar 6 10:17:26 dinhthithanhtam-b22dcat253-virtual-machine systemd-logind[948]: Removed session c1.
Mar 6 10:18:23 dinhthithanhtam-b22dcat253-virtual-machine pxeexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
Mar 6 10:18:23 dinhthithanhtam-b22dcat253-virtual-machine pxeexec[2573]: dinhthithanhtam-b22dcat253: Executing command [USER=root] [TTY=unknown] [CWD=/home/dinhthithanhtam-b22dcat253] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Mar 6 10:21:39 dinhthithanhtam-b22dcat253-virtual-machine sudo: dinhthithanhtam-b22dcat253 : TTY=pts/0 ; PWD=/home/dinhthithanhtam-b22dcat253 ; USER=root ; COMMAND=/usr/bin/systemctl status apache2
Mar 6 10:21:39 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Mar 6 10:21:39 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
Mar 6 10:22:30 dinhthithanhtam-b22dcat253-virtual-machine sudo: dinhthithanhtam-b22dcat253 : TTY=pts/0 ; PWD=/home/dinhthithanhtam-b22dcat253 ; USER=root ; COMMAND=/usr/bin/apt install apache2 -y
Mar 6 10:22:30 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Mar 6 10:23:17 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
Mar 6 10:23:38 dinhthithanhtam-b22dcat253-virtual-machine sudo: dinhthithanhtam-b22dcat253 : TTY=pts/0 ; PWD=/home/dinhthithanhtam-b22dcat253 ; USER=root ; COMMAND=/usr/bin/systemctl status apache2
Mar 6 10:23:38 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Mar 6 10:24:22 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
Mar 6 10:24:22 dinhthithanhtam-b22dcat253-virtual-machine pxeexec[3681]: dinhthithanhtam-b22dcat253: Executing command [USER=root] [TTY=unknown] [CWD=/home/dinhthithanhtam-b22dcat253] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Mar 6 10:26:03 dinhthithanhtam-b22dcat253-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
Mar 6 10:30:01 dinhthithanhtam-b22dcat253-virtual-machine CRON[5232]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 6 10:30:01 dinhthithanhtam-b22dcat253-virtual-machine CRON[5232]: pam_unix(cron:session): session closed for user root
Mar 6 10:33:22 dinhthithanhtam-b22dcat253-virtual-machine pxeexec[5996]: dinhthithanhtam-b22dcat253: Executing command [USER=root] [TTY=unknown] [CWD=/home/dinhthithanhtam-b22dcat253] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Mar 6 10:51:56 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: pam_unix(gdm-password:auth): conversation failed
Mar 6 10:51:56 dinhthithanhtam-b22dcat253-virtual-machine gdm-password: pam_unix(gdm-password:auth): auth could not identify password for [dinhthithanhtam-b22dcat253]
```

- Dùng gawk để lọc và in dữ liệu mong muốn
- Sau khi tìm thấy thông tin bằng grep, ta sử dụng gawk để trích xuất và in nội dung mong muốn. Ví dụ:

```
ssh user@IP_VICTIM "cat /var/log/auth.log | grep 'new user' | gawk '{print \$1, \$2, \$3, \$11}'"
```

- Trong đó:
  - \$1, \$2, \$3: Thời gian tạo user.
  - \$11: Tên tài khoản được tạo.

```
Mar 6 10:15:16 gdm(uid=128)
Mar 6 10:15:32 (system
Mar 6 10:17:01 control
Mar 6 10:17:01 later
Mar 6 10:17:01 dinhthithanhtam-b22dcat253(uid=1000)
Mar 6 10:17:01 dinhthithanhtam-b22dcat253.
Mar 6 10:17:01 dinhthithanhtam-b22dcat253(uid=1000)
Mar 6 10:17:01 root(uid=0)
Mar 6 10:17:01 root
Mar 6 10:17:02 unlocked
Mar 6 10:17:04 initialized
Mar 6 10:17:05 initialized
Mar 6 10:17:05 initialized
Mar 6 10:17:09 (system
Mar 6 10:17:24 gdm
Mar 6 10:17:24 for
Mar 6 10:17:25 (system
Mar 6 10:17:26
Mar 6 10:18:23 root(uid=0)
Mar 6 10:18:23 [CWD=/home/dinhthithanhtam-b22dcat253]
Mar 6 10:21:39 ;
Mar 6 10:21:39 root(uid=0)
Mar 6 10:21:39 root
Mar 6 10:21:39 root
Mar 6 10:22:30 root(uid=0)
Mar 6 10:23:17 root
Mar 6 10:23:38 ;
Mar 6 10:23:38 root(uid=0)
Mar 6 10:24:22 root(uid=0)
Mar 6 10:24:22 [CWD=/home/dinhthithanhtam-b22dcat253]
Mar 6 10:26:03 root
Mar 6 10:30:01 root(uid=0)
Mar 6 10:30:01 root
Mar 6 10:33:22 root(uid=0)
Mar 6 10:33:22 [CWD=/home/dinhthithanhtam-b22dcat253]
Mar 6 10:51:56
Mar 6 10:51:56 password
```

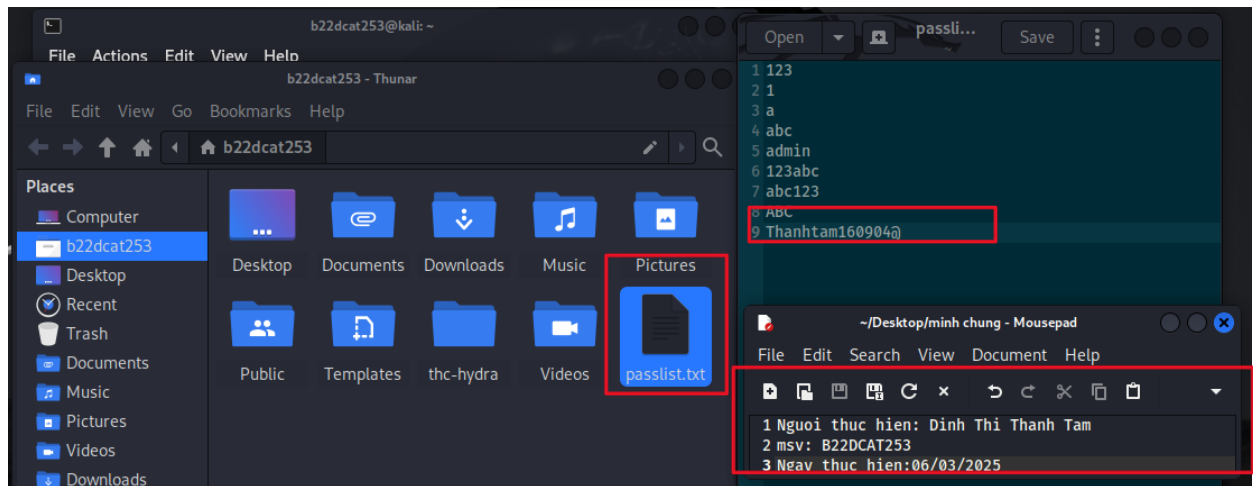
```
1 Người thực hiện: Dinh Thi Thanh Tam
2 msv: B22DCAT253
3 Ngày thực hiện: 04/03/2025
4 == day la may kali linux ==
5
```



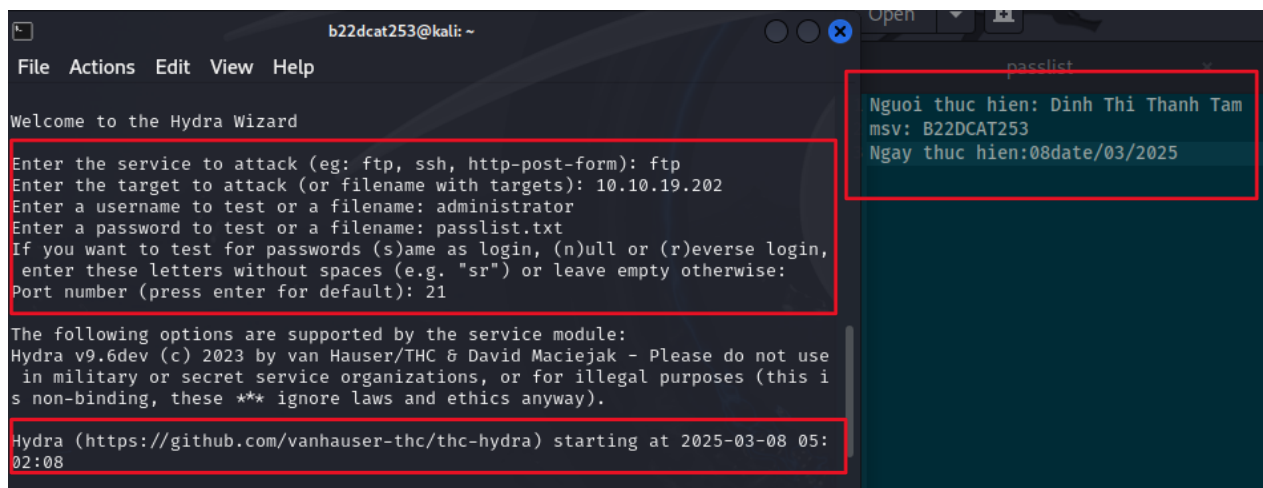
## 2.2.3 Phân tích log sử dụng find trong Windows

### 2.2.3.1 Sử dụng xHydra để brute-force FTP

- Tạo file passlist.txt để lưu trữ các mật khẩu có thể được đặt để quét trên máy nạn nhân đó có 1 mật khẩu đúng để việc thử nghiệm quét được thành công



- Mở terminal trên Kali Linux và mở hydra:
- Nhập target: 10.10.19.202 (ip máy nạn nhân)
- Nhập username: administrator
- Nhập password là danh sách mật khẩu vừa tạo: passlist.txt



- Sau đó tiến hành quét mật khẩu trên máy nạn nhân:

```
b22dcat253@kali: ~  
File Actions Edit View Help  
The following command will be executed now:  
hydra -l administrator -P passlist.txt -u -s 21 10.10.19.202 ftp  
Do you want to run the command now? [Y/n] Y  
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use  
in military or secret service organizations, or for illegal purposes (this i  
s non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-08 05:  
02:10  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1  
try per task  
[DATA] attacking ftp://10.10.19.202:21/  
[21][ftp] host: 10.10.19.202 login: administrator password: ThanhTam16090  
4@  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-08 05:  
02:11  
(b22dcat253@kali)~  
$ date  
Sat Mar 8 05:30:00 AM EST 2025
```

➔ Thành công tìm được mật khẩu nghĩa là cuộc tấn công brute-force đã tìm thấy mật khẩu đúng.

### 2.2.3.2 Phân Tích Log FTP trên Windows Server 2019

Thực hiện phân tích log FTP trên máy Windows Server 2019 External Victim sau khi thử nghiệm brute-force tấn công. Mục tiêu là tìm kết quả đăng nhập thành công từ file log FTP

- Điều hướng đến thư mục chứa log FTP
- Mở Command Prompt (cmd.exe) trên Windows Server 2019
- Điều hướng đến thư mục chứa log của Microsoft FTP Server

*Cd C:\inetpub\log\LogFiles\FTPSVC3*

- Chọn file log có ngày tháng phù hợp với thời điểm thực hiện tấn công. Ngày 08-03-2025
- Để lọc kết quả đăng nhập thành công, tìm mã 230 trong log:

*Find "230" u\_ex250308.log*

```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.17763.3650]  
(c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>cd C:\inetpub\logs\LogFiles\FTPSVC3  
C:\inetpub\logs\LogFiles\FTPSVC3>find "230" u_ex250301.log  
File not found - U_EX250301.LOG  
C:\inetpub\logs\LogFiles\FTPSVC3>find "230" u_ex250308.log  
----- U_EX250308.LOG  
2025-03-08 10:01:36 10.10.19.148 DTTT253\Administrator 10.10.19.202 21 PASS *** 230 0 0 c7c2e29d-e822-4eb2-923f-79eb79cc  
f909 /  
2025-03-08 10:02:08 10.10.19.148 DTTT253\Administrator 10.10.19.202 21 PASS *** 230 0 0 18befad9-3364-438a-a7f2-9ba90979  
a52e /  
C:\inetpub\logs\LogFiles\FTPSVC3>date  
The current date is: Sat 03/08/2025  
Enter the new date: (mm-dd-yy)  
C:\inetpub\logs\LogFiles\FTPSVC3>
```

➔ Mã 230 trong log FTP có nghĩa là đăng nhập thành công.

## KẾT LUẬN

Bài thực hành đã giúp phân tích log hệ thống để xác định dấu vết tấn công. Thông qua các công cụ như grep, gawk trên Linux và find trên Windows, giúp có thể lọc và tìm kiếm dữ liệu liên quan đến cuộc tấn công. Kết quả cho thấy log ghi lại các lần đăng nhập thành công sau tấn công brute-force bằng Hydra. Dữ liệu log này được lưu lại để phục vụ phân tích bảo mật.

## TÀI LIỆU THAM KHẢO

- [1] grep: [https://linuxcommand.org/lc3\\_man\\_pages/grep1.html](https://linuxcommand.org/lc3_man_pages/grep1.html)
- [2] gawk: <http://www.gnu.org/software/gawk/manual/gawk.html>
- [3] find: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>
- [4] xhydra: <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>